INTERNATIONAL STANDARD

ISO/IEC 15408-4

First edition
2022-08

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

Part 4: Framework for the specification of evaluation methods and activities

Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information —

Partie 4: Cadre prévu pour la spécification des méthodes d'évaluation et des activités connexes

Reference number
ISO/IEC 15408-4:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 15408 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Legal notice

The governmental organizations listed below contributed to the development of this version of the Common Criteria for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations (called CC), they hereby grant non-exclusive license to ISO/IEC to use CC in the continued development/maintenance of the ISO/IEC 15408 series of standards. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC as they see fit.

Australia	The Australian Signals Directorate
Canada	Communications Security Establishment
France	Agence Nationale de la Sécurité des Systèmes d'Information
Germany	Bundesamt für Sicherheit in der Informationstechnik
Japan	Information-technology Promotion Agency
Netherlands	Netherlands National Communications Security Agency
New Zealand	Government Communications Security Bureau
Republic of Korea	National Security Research Institute
Spain	Ministerio de Asuntos Económicos y Transformación Digital
Sweden	FMV, Swedish Defence Materiel Administration
United Kingdom	National Cyber Security Centre
United States	The National Security Agency

Introduction

The ISO/IEC 15408 series permits comparability between the results of independent security evaluations, by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. ISO/IEC 18045 provides a companion methodology for some of the assurance requirements specified in the ISO/IEC 15408 series.

The model of security evaluation in ISO/IEC 15408-1 identifies that high-level generic evaluation activities are defined in ISO/IEC 18045, but that more specific evaluation activities (EAs) can be defined as technology-specific adaptations of these generic activities for particular evaluation contexts, e.g. for security functional requirements (SFRs)or security assurance requirements (SARs) applied to specific technologies or target of evaluation (TOE) types. Specification of such evaluation activities is already occurring amongst practitioners and this creates a need for a specification for defining such evaluation activities.

This document describes a framework that can be used for deriving evaluation activities from work units of ISO/IEC 18045 and grouping them into evaluation methods (EMs). Evaluation activities or evaluation methods can be included in protection profiles (PPs) and any documents supporting them. Where a PP, PP-Configuration, PP-Module, package, or Security Target (ST) identifies that specific evaluation methods/evaluation activities are to be used, then the evaluators are required by ISO/IEC 18045 to follow and report the relevant evaluation methods/evaluation activities when assigning evaluator verdicts. As noted in ISO/IEC 15408-1, in some cases an evaluation authority can decide not to approve the use of particular evaluation methods/evaluation activities: in such a case, the evaluation authority can decide not to carry out evaluations following an ST that requires those evaluation methods/evaluation activities.

This document also allows for evaluation activities to be defined for extended SARs, in which case derivation of the evaluation activities relates to equivalent action elements and work units defined for that extended SAR. Where reference is made in this document to the use of ISO/IEC 18045 or ISO/IEC 15408-3 for SARs (such as when defining rationales for evaluation activities), then, in the case of an extended SAR, the reference applies instead to the equivalent action elements and work units defined for that extended SAR.

For clarity, this document specifies how to define evaluation methods and evaluation activities but does not itself specify instances of evaluation methods or evaluation activities.

The following NOTE appears in other parts of the ISO/IEC 15408 series and in ISO/IEC 18045 to describe the use of bold and italic type in those documents. This document does not use those conventions, but the NOTE has been retained for alignment with the rest of the series.

NOTE This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type.

The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation.

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

Part 4: Framework for the specification of evaluation methods and activities

1 Scope

This document provides a standardized framework for specifying objective, repeatable and reproducible evaluation methods and evaluation activities.

This document does not specify how to evaluate, adopt, or maintain evaluation methods and evaluation activities. These aspects are a matter for those originating the evaluation methods and evaluation activities in their particular area of interest.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information security, cybersecurity and privacy protection — Methodology for IT security evaluation*

3 Terms and definitions

For the purposes of this document, the terms and definitions in ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, and ISO/IEC 18045 apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

4 General model of evaluation methods and evaluation activities

4.1 Concepts and model

ISO/IEC 18045 defines a generic set of work units that an evaluator carries out in order to reach a verdict for most of the assurance classes, families and components defined in ISO/IEC 15408-3. The

relationship between the structure of a SAR in ISO/IEC 15408-3 and the work units in ISO/IEC 18045 is described in ISO/IEC 18045 and summarized in Figure 1.

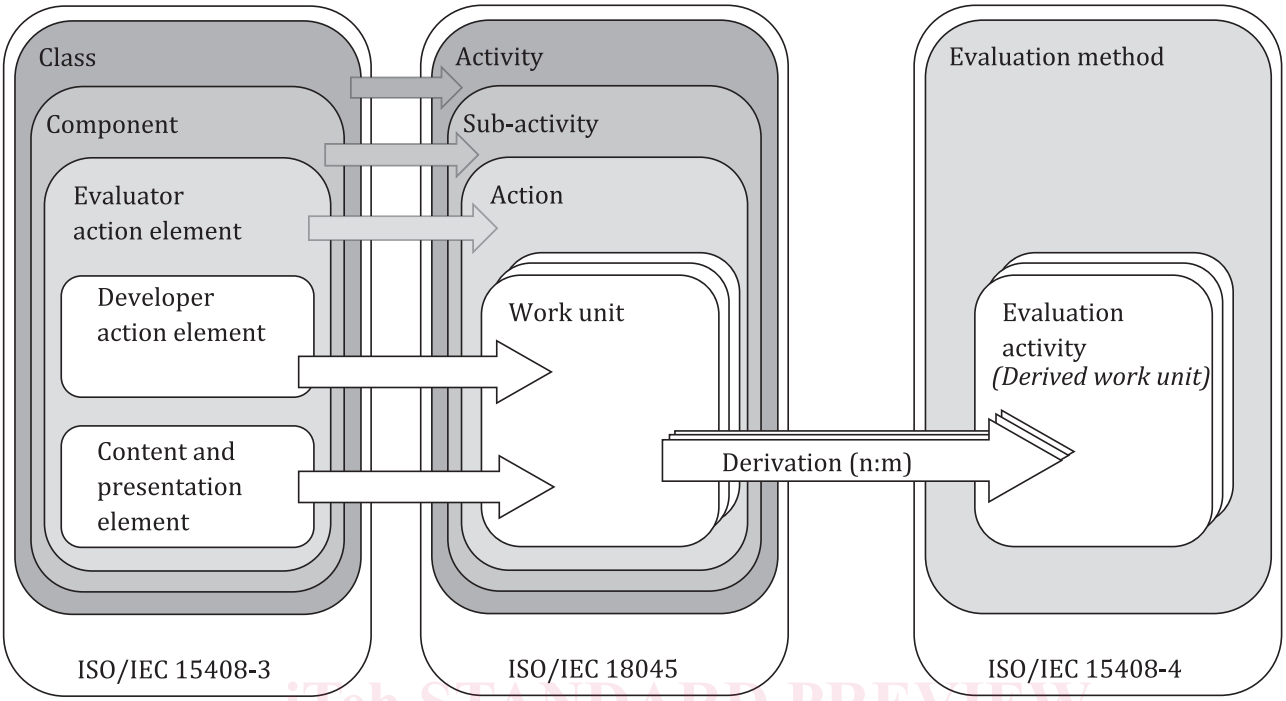

Figure 1 — Mapping of ISO/IEC 15408-3 and ISO/IEC 18045 structures to structures of this document

For the purposes of defining new evaluation methods and evaluation activities, the main point to note is that each action (representing an evaluator action element in ISO/IEC 15408-3 or an implied evaluator action element) is represented in ISO/IEC 18045 as a set of work units that are carried out by an evaluator.

This document specifies the ways in which new evaluation activities can be derived from the generic work units in ISO/IEC 18045, and combined into an evaluation method that is intended for use in some particular evaluation context. A typical example of such an evaluation context would be a particular TOE type or particular technology type.

EXAMPLE 1

TOE type: a network device

Technology type: specific cryptographic functions

If evaluation methods and evaluation activities are required to be used with a particular PP, PP-Module, PP-Configuration, then a PP or PP-Module or PP-Configuration shall identify this requirement in its conformance statement. If evaluation methods and evaluation activities are required to be used with a particular package, then the package shall identify this requirement in the security requirement section. If Evaluation Methods and Evaluation Activities are claimed by an ST as a result of that ST claiming conformance to a PP, PP-Configuration, or package, then the ST shall identify the EMs/EAs used in its conformance claim. No formal claim of conformance to ISO/IEC 15408-4 is made in any of these cases (the contents of PPs, PP-Modules, PP-Configurations and packages are described in more detail in ISO/IEC 15408-1).

A PP, PP-Configuration, PP-Module or package may use more than one evaluation method or separate set of evaluation activities.

EXAMPLE 2 Multiple evaluation methods can be used where separate evaluation methods have been defined for cryptographic operations and for secure channel protocols used in a PP.

NOTE Where exact conformance is used, ISO/IEC 15408-1 states that evaluation methods/evaluation activities are not allowed to be defined in a PP-Configuration: the evaluation methods/evaluation activities to be used are included in the PPs and PP-Modules and not in the PP-Configuration).

When a PP, PP-Module, PP-Configuration, or package identifies that certain evaluation methods/ evaluation activities are to be used, then this is done using a standard wording that states the requirement and references the definition of the evaluation methods/evaluation activities to be used. An ST shall only identify required evaluation methods and evaluation activities that are included in a PP, PP-Module, PP-Configuration or package to which the ST claims conformance (i.e. the ST itself shall not add, modify or remove any evaluation methods or evaluation activities). An ST shall include identification of all evaluation methods/evaluation activities that it requires (i.e. including any that are required by PPs, PP-Modules, PP-Configurations, or packages to which the ST claims conformance), so that there is a single list that can be checked and referenced by evaluators and readers of the ST.

Evaluation methods and evaluation activities may be defined within the document that requires them (e.g. as part of a PP), or externally in a different document (or in a combination of both). Although identification is required as described above, it is not necessary to reproduce the text of the evaluation methods/evaluation activities in other documents (e.g, an ST does not have to include the full text of the evaluation methods/evaluation activities from a PP to which it claims conformance).

4.2 Deriving evaluation methods and evaluation activities

In general, defining evaluation activities and evaluation methods may start either from an SAR, aiming to make some or all parts of its work units more specific, or from an SFR, aiming to define specific aspects of work units related to that SFR.

When starting from an SAR, a guideline for the process is as follows.

a) Identify the relevant ISO/IEC 18045 work units from which to derive at least one individual evaluation activity or groups of evaluation activities.

b) For each work unit from which an evaluation activity is derived:

   1) define the new evaluation activities in terms of the specific work to be carried out and evaluation criteria as described in 6.2 (including, if required, pass/fail criteria as described in 6.2.8);

   2) group evaluation activities into an evaluation method if necessary;

   3) state the rationale for the new evaluation activities and the evaluation method under which they are grouped as described in 5.2.10 and 6.2.10.

      EXAMPLE A rationale can include reference to the developer action, and content and presentation elements of the work units from which they are derived.

A guideline for starting from an SFR would be as follows.

a) Identify the relevant SFR.

b) Identify the SARs (from ISO/IEC 15408-3 or a set of extended SARs, or both) to be addressed for that particular SFR, and the corresponding ISO/IEC 18045 work units.

c) Define the new evaluation activities in terms of the specific work to be carried out and evaluation criteria as described in 6.2 (including, if required, pass/fail criteria as described in 6.2.8).

   EXAMPLE Evaluation activities can be defined to examine the presentation of a specific SFR in the TOE Summary Specification (derived from ASE), to examine the presentation of the SFR in the guidance documentation (derived from AGD), and to carry out specific tests of the SFR (derived from ATE).

d) Map the affected work units for the SARs to the new evaluation activities.

e) State the rationale for the new evaluation activities, and the evaluation method under which they are grouped, as described in 5.2.10 and 6.2.10.

Although an author may choose to start from SARs or SFRs, it is noted that SARs ultimately cover all SFRs. Starting from SFRs as described above is a technique that can be useful when clarifying the detail of how an SAR applies to a particular SFR, and that can be useful for presenting SFRs alongside the description of their evaluation activities.

It is not required to have a 1:1 mapping between work units and new evaluation activities, and the actual correspondence is documented in a rationale (as described in 5.2.10). The derivation may be made in terms of individual work units or groups of work units, and this is depicted in Figure 2. In case a) of Figure 2 the author maps each work unit from ISO/IEC 18045 to a corresponding evaluation activity, while in case b) the author maps different numbers of work units and evaluation activities, whilst still addressing all aspects of an action (i.e. the collection of work units).

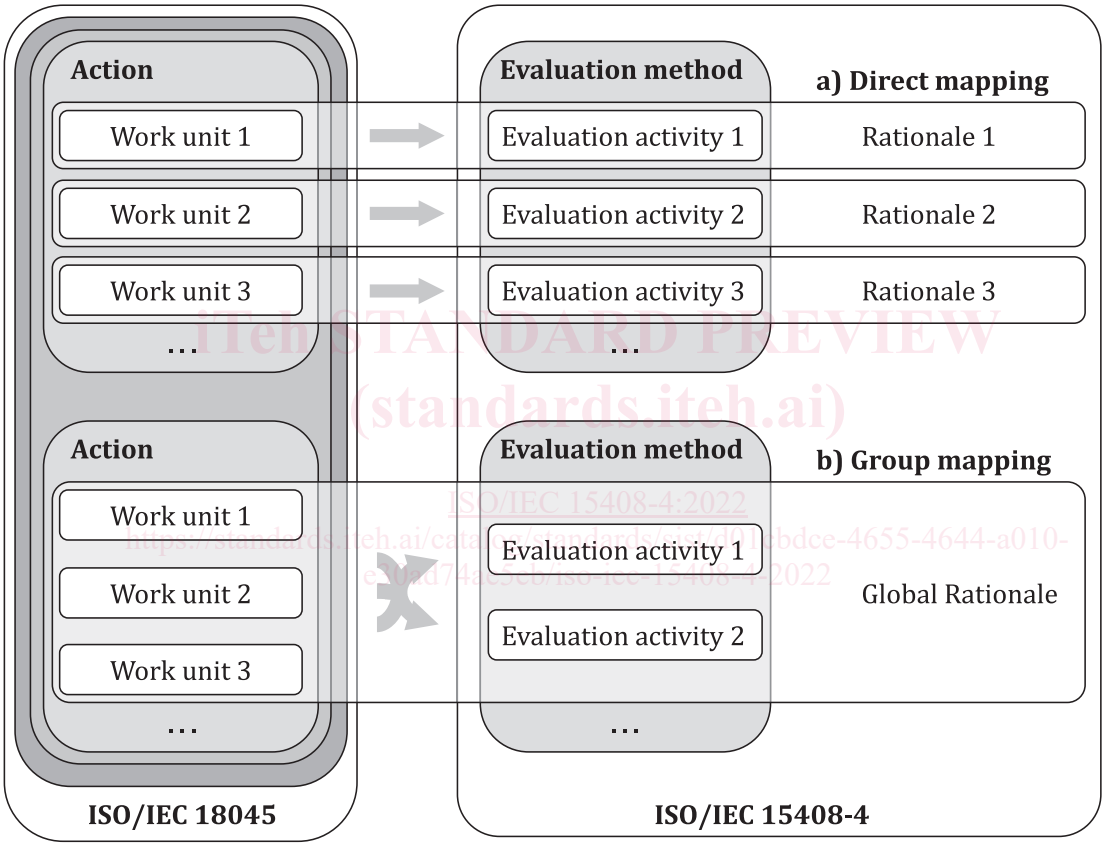

Figure 2 — Alternative approaches to mapping ISO/IEC 18045 to derived evaluation activities

Other approaches are possible depending on the content of the specific work units and evaluation activities: even where the same number of work units and evaluation activities exist, a simple 1:1 mapping is sometimes not possible and therefore a mapping at the action level may be appropriate. Some more detailed mapping situations are described in the examples below.

NOTE These examples assume that the evaluation activities described are being defined by a community that can judge the suitability of the rationale for completeness of the evaluation activities. The examples are concerned only with the form and structure of the mappings, not with the nature or acceptance of the completeness rationale.

EXAMPLE 1

For a TOE type that includes both software and hardware, additional evaluation activities can be defined to deal with the manufacturing environment and its processes. Considering the ALC_DVS family, a possible approach would be to adopt all the existing ALC_DVS work units for the software development environment and to define additional evaluation activities for each of the relevant hardware and manufacturing aspects. These aspects can include extensions of the normal ALC_DVS scope to additional items such as protection of hardware design in the development environment, secure transfer of software from the development environment to the manufacturing environment, security of the manufacturing site, and protection of the manufactured product while awaiting delivery. They can also include new aspects related to objects and processes that arise only in the manufacturing environment, such as:

— confirming that the firmware used on a manufacturing line is reliably obtained from the authorized version created on the firmware build system;

— checking configuration management of test programs for testing the TOE on the manufacturing line;

— confirming that processes to disable test or debug interfaces on the TOE operate correctly and reliably;

— examining the physical and logical security of key management systems used to inject keys or certificates into the TOE during manufacture.

In this example the original ALC_DVS.1.1E action is mapped to include all the new evaluation activities, but an alternative approach would be to define additional evaluation activities for each individual work unit for ALC_DVS.1E, identifying the additional activities to cover the manufacturing environment for that work unit.

EXAMPLE 2

If AVA_VAN.1 vulnerability analysis is applied to a particular type of TOE, where there is a specific need to achieve consistency in the public domain vulnerability sources used then a possible approach would be to define an evaluation activity that covers the AVA_VAN work unit dealing with searching public domain sources by specifying the particular sources to be used, perhaps along with particular searches to be carried out and decision criteria for selecting a resulting list of potential vulnerabilities to be analysed and tested. In this example the original AVA_VAN.1-3 work unit is mapped to the new evaluation activity.

EXAMPLE 3

For an evaluation method to be used with hardware such as an integrated circuit, evaluation activities can be defined to examine the circuit's architecture, defining required inputs that give the evaluator specific details about the operations and information available through the circuit’s interfaces. The definition of these required inputs can then make clear that the relevant interfaces include the circuit's physical surface, its executable programming instructions, and its communication interfaces.

Further evaluation activities within the evaluation method can examine the circuit's resistance against physical probing in order to prevent manipulating or disabling TSF features.

For testing activities, evaluation activities within the evaluation method can define a required input that presents the circuit's design as a flow chart of security functions permeating through the circuit's subsystems. The flow chart can then be used by the evaluator to create test cases and to confirm the test coverage of the circuit.

EXAMPLE 4

For a TOE type such as a network device that provides cryptographically verifiable firmware updates, evaluation activities can give specific details of how the evaluator is required to review the Security Target and guidance documentation to confirm certain specific characteristics required of the cryptographic update process.

Other evaluation activities can define specific test cases covering the verification of the current firmware, the availability of updates, fetching updates, verifying the source of the updates using cryptographic signatures, and the use of specific types of invalid update in order to test the TOE's acceptance functions.

4.3 Verb usage in the description of evaluation methods and evaluation activities

Where a verb is defined in ISO/IEC 15408-1 then the description of evaluation activities shall use those verbs only in accordance with the definitions. Alternative verbs may be used in an evaluation method for use in its evaluation activities provided that the alternative verbs are defined in the evaluation